

IN THE ABSTRACT:

Please delete the Abstract as originally filed:

4 The present invention provides systems, apparatus and methods for providing
5 cryptographic keys which are usable in a network of connected computer nodes applying
6 a signature scheme. Further, the present invention provides systems, apparatus and
7 methods for providing a signature value on a message in a network of connected
8 computer nodes, and systems, apparatus and methods for verifying the signature value on
9 the message.

10 [Fig. 2]

Please replace the Abstract of the invention with the following:

-- A system and method for providing cryptographic keys which are usable in a network of connected computer nodes applying a signature scheme. The method employs: generating a random secret key usable in the network of connected computer nodes; generating an exponent interval I having a plurality of exponent elements, the exponent interval having a specified first random limit, wherein each element of the plurality of exponent elements of the exponent interval has a unique prime factor that is larger than a given security parameter; and, providing a public key comprising an exponent-interval description including the first random limit, and a public key value derived from the random secret key, such that the random secret key and a selected exponent value from the plurality of exponent elements in the exponent interval I are usable for deriving a signature value on a message to be sent within the network to a second computer node for verification.--